Conditional SIC-POVMs

Dénes Petz[1], László Ruppert[2] and András Szántó [3]

Department of Mathematical Analysis,
Budapest University of Technology and Economics,
Egry József u. 1., Budapest, 1111 Hungary

Abstract

In this paper we examine a generalization of the symmetric informationally complete POVMs. SIC-POVMs are the optimal measurements for full quantum tomography, but if some parameters of the density matrix are known, then the optimal SIC POVM should be orthogonal to a subspace. This gives the concept of the conditional SIC-POVM. The existence is not known in general, but we give a result in the special cases when the diagonal is known of the density matrix.

Keywords: Quantum state tomography, Hilbert-Schmidt distance, SIC-POVM, projections, quasi-orthogonality.

AMS 2010 Subject Classification: Primary 81P15; Secondary 94A15.

1 Introduction

The motivation for a positive operator valued measure (POVM) is in the quantum information theory. The outcome statistics of a quantum measurement are described by (one or more) POVMs. A sequence of measurements on copies of a system in an unknown state will reveal the state. This process is called quantum state tomography [10].

A POVM is a set $\{E_i : 1 \le i \le k\}$ of positive operators such that $\sum_i E_i = I$. A quantum density matrix ρ can be informed by the probability distribution $\{\mathrm{Tr}\, \rho E_i : 1 \le i \le k\}$. A density $\rho \in M_n(\mathbb{C})$ has $n^2 - 1$ real parameters. To cover all parameters $k \ge n^2$ should hold for the POVM. We can take projections P_i, $1 \le i \le n^2$, such that

$$\sum_{i=1}^{n^2} P_i = nI, \qquad \mathrm{Tr}\, P_i P_j = \frac{1}{n+1} \quad (i \ne j), \qquad E_i = \frac{1}{n} P_i$$

and this is called symmetric informationally complete POVM (SIC POVM) by Zauner [18] and it is rather popular now [1, 2, 4, 9, 14, 19]. Zauner shoved the existence for $n \le 5$

[1]E-mail: petz@math.bme.hu
[2]E-mail: ruppertl@gmail.com
[3]E-mail: prikolics@gmail.com

and there has been more mathemtical and numerical arguments [6, 16]. The existence of a SIC POVM is not known for every dimension. Another terminology for this is tight equiangular frame. We may also consider less than n^2 projections with similar properties.

A SIC POVM $\{E_i : 1 \le i \le n^2\}$ of an n-level system is optimal for several arguments. For example, the SIC POVM was optimal in our paper [12] where the minimization of the determinant of the average covariance matrix was studied. Actually, this kind of optimization is too complicated and a different argument was in [15], minimization of the square of the Hilbert-Schmidt distance of the estimation and the true density. In the present paper the minimization of the square of the Hilbert-Schmidt distance will be used.

In this paper the subject is the state estimation again, but a part of the n^2-1 parameters is supposed to be known and we want to estimate only the unknown parameters. A POVM $\{E_i : 1 \le i \le k\}$ is good when $k < n^2$ and n^2-k parameters are known. It is obvious that the optimal POVM depends on the known parameters and we use the expression of conditional SIC POVM. This seems to be a new subject, the existence of such conditional SIC POVM can be a fundamental question in different quantum tomography problems. The description of the conditional SIC POVM is the main result in Section 1, however, the existence is not at all clear. The formalism is in a finite dimensional Hilbert space $\mathcal{H}$ and a state means a density matrix in $B(\mathcal{H})$. The known parameters determine a traceless part $B \subset B(\mathcal{H})$ and the operators of the conditional SIC POVM are orthogonal to B. In Section 2 a particular situation is studied, we assume that the diagonal entries of the state space are given. A mathematical subject called planar difference set in projective geometry is used there.

2 The optimality of conditional SIC-POVMs

We examine the case of $M_n(\mathbb{C})$. Let us suppose that σ_i is an orthonormal basis of self-adjoint matrices, i.e.

$$\sigma_i = \sigma_i^*, \quad \langle \sigma_i, \sigma_j \rangle = \delta_{i,j}, \quad i, j \in \{0, 1, 2, \dots n^2-1\}.$$

We fix $\sigma_0 = \frac{1}{\sqrt{n}} I_n$. (The elements of this basis are often called generalized Pauli matrices.)

A quantum state ρ satisfies the conditions $\mathrm{Tr}\,\rho = 1$ and $\rho \ge 0$. It can be written in the form

$$\rho = \sum_{i=0}^{n^2-1} \theta_i \sigma_i,$$

where $\theta_0 = \frac{1}{\sqrt{n}}$. A necessary condition for the coefficients can be obtained:

$$\sum_{i=1}^{n^2} \theta_i^2 = \mathrm{Tr}\,\rho^2 \le 1. \tag{1}$$

We decompose $M_n(\mathbb{C})$ to three orthogonal subspaces:

$$M_n(\mathbb{C}) = A \oplus B \oplus C, \tag{2}$$

where $A := \{\lambda I_n : \lambda \in \mathbb{C}\}$ is one dimensional. Denote the orthogonal projections to the subspaces A, B, C by $\mathbf{A}, \mathbf{B}, \mathbf{C}$. A density matrix $\rho \in M_n(\mathbb{C})$ has the form

$$\rho = \frac{I_n}{n} + \mathbf{B}\rho + \mathbf{C}\rho.$$

Assume that $\mathbf{B}\rho$ is the known traceless part of ρ and $\mathbf{C}\rho$ is the unknown traceless part of ρ. We use the notation $\rho_* = \rho - \mathbf{B}\rho$. The aim of the state estimation is to cover ρ_*. If the dimension of B is m, then the dimension of C is $n^2 - m - 1$. For the state estimation we have to use a POVM with at least $N = n^2 - m$ elements. To get a unique solution we will use POVM with exactly N elements: $\{F_1, F_2, \dots, F_N\}$. For obtaining optimal POVM, we will use similar arguments to [11] which was a straightforward extension of the idea appeared in [15].

If $\{Q_i : 1 \le i \le N\}$ are self-adjoint matrices satisfying the following equation

$$\rho_* = \frac{1}{n} I + \sum_{\sigma_i \in C} \theta_i \sigma_i = \sum_{i=1}^{N} p_i Q_i, \qquad p_i = \mathrm{Tr}\, \rho F_i,$$

then $\{Q_i : 1 \le i \le N\}$ is a **dual frame** of $\{F_i : 1 \le i \le N\}$. Then the state reconstruction formula can be written as

$$\hat{\rho_*} = \sum_{i=1}^{N} \hat{p}_i Q_i.$$

We define the distance as

$$\|\rho_* - \hat{\rho_*}\|_2^2 = \mathrm{Tr}\, (\rho_* - \hat{\rho_*})^2 = \sum_{i,j=1}^{N} (p(i) - \hat{p}(i))(p(j) - \hat{p}(j)) \langle Q_i, Q_j \rangle$$

and its expectation value is

$$\begin{aligned} &\sum_{i,j=1}^{N} (p(i)\delta(i,j) - p(i)p(j)) \langle Q_i, Q_j \rangle \\ &= \sum_{i=1}^{N} p(i) \langle Q_i, Q_i \rangle - \langle \sum_{i=1}^{N} p(i) Q_i, \sum_{j=1}^{N} p(j) Q_j \rangle \\ &= \sum_{i=1}^{N} p(i) \langle Q_i, Q_i \rangle - \mathrm{Tr}\, (\rho_*)^2. \end{aligned}$$

We concentrate on the first term which is

$$\sum_{i=1}^{N} (\mathrm{Tr}\, F_i \rho) \langle Q_i, Q_i \rangle \tag{3}$$

and we take the integral with respect to the Haar measure on the unitaries $\mathrm{U}(n)$.

Note first that

$$\int_{\mathrm{U}(n)} UPU^*\ d\mu(U)$$

is the same constant c for any projection of rank 1. If $\sum_{i=1}^n P_i = I_n$, then

$$nc = \sum_{i=1}^n \int_{\mathrm{U}(n)} UP_iU^*\ d\mu(U) = I_n$$

and we have $c = I_n/n$. Therefore for $A = \sum_{i=1}^n \lambda_i P_i$ we have

$$\int_{\mathrm{U}(n)} UAU^*\ d\mu(U) = \sum_{i=1}^n \lambda_i c = \frac{I_n}{n} \mathrm{Tr}\, A$$

and application to the integral of (3) gives

$$\int \mathrm{Tr}\, F_i(U\rho U^*)\, d\mu(U) = \frac{1}{n} \mathrm{Tr}\, F_i.$$

So we get the following quantity for the error of the state estimation:

$$T := \int E\left(\|U\rho^*U^* - U\hat{\rho^*}U^*\|_2^2\right) d\mu(U) = \frac{1}{n}\sum_{i=1}^N (\mathrm{Tr}\, F_i)\langle Q_i, Q_i\rangle - \mathrm{Tr}\,(\rho^*)^2$$

This is to be minimized. Since the second part is constant, our task is to minimize the first part:

$$\sum_{i=1}^N (\mathrm{Tr}\, F_i)\langle Q_i, Q_i\rangle \tag{4}$$

We define the superoperator:

$$\mathbf{F} = \sum_{i=1}^N |F_i\rangle\langle F_i| (\mathrm{Tr}\, F_i)^{-1}.$$

It will have rank N, so if $N < n^2$ the inverse of $\mathbf{F}$ does not exists, but we can use its pseudo-inverse $\mathbf{F}^-$, so $\mathbf{F}^-|\sigma_i\rangle = 0$, if $\sigma_i \in B$. R_i is the canonical dual frame of F_i, if

$$|R_i\rangle = \mathbf{F}^-|P_i\rangle,$$

where $P_i = (\mathrm{Tr}\, F_i)^{-1} F_i$.

Lemma 1 *For a fixed F_i, (4) is minimal if $Q_i = R_i$, i.e. if we use the canonical dual frame.*

Proof. Let us use the notation $W_i = Q_i - R_i$. Then

$$\begin{aligned}
\sum_{i=1}^{N} \operatorname{Tr} F_i |R_i\rangle\langle W_i| &= \sum_{i=1}^{N} \operatorname{Tr} F_i |R_i\rangle\langle Q_i| - \sum_{i=1}^{N} \operatorname{Tr} F_i |R_i\rangle\langle R_i| \\
&= \sum_{i=1}^{N} \operatorname{Tr} F_i \mathbf{F}^{-} |P_i\rangle\langle Q_i| - \sum_{i=1}^{N} \operatorname{Tr} F_i \mathbf{F}^{-} |P_i\rangle\langle P_i| \mathbf{F}^{-} \\
&= \mathbf{F}^{-} \sum_{i=1}^{N} \operatorname{Tr} F_i |P_i\rangle\langle Q_i| - \mathbf{F}^{-} \Big(\sum_{i=1}^{N} \operatorname{Tr} F_i |P_i\rangle\langle P_i| \Big) \mathbf{F}^{-} \\
&= \mathbf{F}^{-}\mathbf{\Pi} - \mathbf{F}^{-}\mathbf{F}\mathbf{F}^{-} = \mathbf{F}^{-}\mathbf{\Pi} - \mathbf{F}^{-}\mathbf{\Pi} = 0,
\end{aligned} \tag{5}$$

where $\mathbf{\Pi} = \mathbf{A} + \mathbf{C}$, and we use that from

$$|\rho^*\rangle = \sum_{i=1}^{N} \langle F_i||\rho\rangle |Q_i\rangle$$

follows

$$\mathbf{\Pi} = \sum_{i=1}^{N} |Q_i\rangle\langle F_i|.$$

So we have

$$\begin{aligned}
\sum_{i=1}^{N} \operatorname{Tr} F_i \langle Q_i, Q_i\rangle &= \sum_{i=1}^{N} \operatorname{Tr} F_i \langle W_i, W_i\rangle + \sum_{i=1}^{N} \operatorname{Tr} F_i \langle W_i, R_i\rangle \\
&\quad + \sum_{i=1}^{N} \operatorname{Tr} F_i \langle R_i, W_i\rangle + \sum_{i=1}^{N} \operatorname{Tr} F_i \langle R_i, R_i\rangle \\
&= \sum_{i=1}^{N} \operatorname{Tr} F_i \langle W_i, W_i\rangle + \sum_{i=1}^{N} \operatorname{Tr} F_i \langle R_i, R_i\rangle \\
&\geq \sum_{i=1}^{N} \operatorname{Tr} F_i \langle R_i, R_i\rangle .
\end{aligned}$$

□

We know the optimal dual frame for a fixed POVM F_i, and the following lemma provides a property for the optimal POVM:

Lemma 2 *The quantity in (4) is minimal if*

$$\mathbf{F} = \mathbf{A} + \frac{n-1}{N-1}\mathbf{C}.$$

Proof. From (5) we have

$$\sum_{i=1}^{N} (\operatorname{Tr} F_i) |R(i)\rangle\langle R(i)| = \mathbf{F}^{-}\mathbf{\Pi} = \mathbf{F}^{-},$$

so we have the equation:

$$\sum_{i=1}^{N} (\mathrm{Tr}\, F_i)\langle R(i), R(i)\rangle = \mathrm{Tr}\,(\mathbf{F}^{-}).$$

Let $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_{n^2}$ be the eigenvalues of $\mathbf{F}$. Since the rank of $\mathbf{F}$ is N, we have $\nu_i = 0$ for $i > N$. We want to minimize

$$\mathrm{Tr}\,(\mathbf{F}^{-}) = \sum_{i=1}^{N} \frac{1}{\nu_i}.$$

It is easy to check that $\mathbf{A}$ is an eigenfunction of $\mathbf{F}$ with $\nu_1 = 1$ eigenvalue:

$$\mathbf{F}|I\rangle = \sum_{i=1}^{N} (\mathrm{Tr}\, F_i)|P(i)\rangle\langle P(i), I\rangle = \sum_{i=1}^{N} (\mathrm{Tr}\, F_i)|P(i)\rangle = \sum_{i=1}^{N} |F(i)\rangle = |I\rangle$$

and we have the following condition:

$$\sum_{i=1}^{N} \nu_i = \mathrm{Tr}\,\mathbf{F} = \sum_{i=1}^{N} \langle P_i, P_i\rangle \mathrm{Tr}\, F_i \leq \sum_{i=1}^{N} \mathrm{Tr}\, F_i = \mathrm{Tr}\, I = n.$$

Combining these conditions we get that the measurement is optimal if $\nu_2 = \nu_3 = \ldots = \nu_N = \frac{n-1}{N-1}$. □

Now we can obtain that the optimal POVM is a conditional SIC-POVM:

Theorem 1 *If*

$$\mathbf{F} = \mathbf{A} + \frac{n-1}{N-1}\mathbf{C}. \tag{6}$$

then

$$\sum_{i=1}^{N} P_i = \frac{N}{n} I, \qquad \mathrm{Tr}\, P_i P_j = \frac{N-n}{n(N-1)} \quad (i \neq j), \qquad \mathrm{Tr}\, \sigma_k P_i = 0 \quad (\sigma_k \in B).$$

Proof. Let us use notation $\lambda_i = \mathrm{Tr}\, F_i$, then (6) has the form:

$$\sum_{i=1}^{N} \lambda_i |P_i\rangle\langle P_i| = \mathbf{A} + \frac{n-1}{N-1}\mathbf{C}.$$

Then we have to the following equation:

$$\sum_{i=1}^{N} \lambda_i \langle Q|P_i\rangle\langle P_i|Q\rangle = \langle Q|\mathbf{A} + \frac{n-1}{N-1}\mathbf{C}|Q\rangle \tag{7}$$

with $Q := P_k - d \cdot I$.

From $\langle P_i | Q \rangle = \mathrm{Tr}\, P_i P_k - d$ the left hand side of (7) becomes

$$\sum_{i=1}^{N} \lambda_i \langle Q|P_i\rangle\langle P_i|Q\rangle = \lambda_k (1-d)^2 + \sum_{i\neq k} \lambda_i (\mathrm{Tr}\, P_i P_k - d)^2.$$

We can compute the right hand side as well:

$$\mathbf{A}(P_k - dI) = \mathbf{A}P_k - dI = \mathbf{A}(P_k - I/n) + I/n - dI = I(1/n - d),$$

$$\langle Q|\mathbf{A}|Q\rangle = (1/n - d)\mathrm{Tr}\,(P_k - dI) = n(1/n-d)^2$$

When $P_k = \sum_{i=0}^{N} c_i \sigma_i$, then

$$\mathbf{C}|Q\rangle = \sum_{\sigma_i \in C} c_i \sigma_i, \qquad \langle Q|\mathbf{C}|Q\rangle = \sum_{\sigma_i \in C} c_i^2.$$

So (7) becomes

$$\lambda_k (1-d)^2 + \sum_{i\neq k} \lambda_i (\mathrm{Tr}\, P_i P_k - d)^2 = n(1/n-d)^2 + \frac{n-1}{N-1} \sum_{\sigma_i \in C} c_i^2. \tag{8}$$

From (1) we have

$$\sum_{\sigma_i \in C} c_i^2 \leq 1 - c_0^2 = 1 - 1/n. \tag{9}$$

This implies

$$\lambda_k (1-d)^2 \leq n(1/n-d)^2 + \frac{n-1}{N-1}(1-1/n),$$

which is true for every value of d, so

$$\lambda_k \leq \min_d \frac{n(1/n-d)^2 + \frac{n-1}{N-1}(1-1/n)}{(1-d)^2}$$

By differentiating we can obtain that the right hand side is minimal if:

$$d = \frac{N-n}{n(N-1)}$$

and then we get

$$\lambda_k \leq \frac{n}{N}.$$

Since $\sum_{i=k}^{N} \lambda_k = n$, we have $\lambda_1 = \lambda_2 = \ldots = \lambda_N = n/N$.

From that follows that there is an equality in (9) too, so we have

$$\sum_{\sigma_i \in C} c_i^2 = 1 - c_0^2 \quad \Rightarrow \quad c_i = 0, \text{ if } \sigma_i \in B \quad \Rightarrow \quad \mathrm{Tr}\, \sigma_i P_k = 0, \text{ if } \sigma_i \in B.$$

On the other hand from (8) we have

$$\sum_{i \neq k} \frac{n}{N} \Big(\mathrm{Tr}\, P_i P_k - \frac{N-n}{n(N-1)} \Big)^2 = 0.$$

So it implies

$$\mathrm{Tr}\, P_i P_k = \frac{N-n}{n(N-1)} \quad \text{if} \quad i \neq k.$$

□

One has to be careful about this result though, since we only consider the case of linear state reconstruction, as it was stated in [15]. Finding the optimal statistic in a more general setting requires complicated nonlinear optimalization.

Now we look at some examples related to the previous theorem and we take different N values.

Example 1 If we do not have any information a priori about the state ($m = 0, N = n^2$), then

$$\mathrm{Tr}\, P_i P_j = \frac{1}{n+1} \quad (i \neq j)$$

so the optimal POVM is the well-known SIC-POVM (if it exists [14]).

Example 2 If we know the off-diagonal elements of the state, and we want to estimate the diagonal entries ($m = n^2 - n, N = n$), then from Theorem 1 it follows that the optimal POVM has the properties

$$\mathrm{Tr}\, P_i P_j = 0 \quad (i \neq j), \quad \sum_{i=1}^{n} P_i = I, \quad \text{and} \quad P_i \text{ is diagonal.}$$

So the diagonal matrix units form an optimal POVM. □

Example 3 If we know the diagonal elements of the state, and we want to estimate the off-diagonal entries ($m = n - 1, N = n^2 - n + 1$), then from Theorem 1 it follows that the optimal POVM has the properties

$$\mathrm{Tr}\, P_i P_j = \frac{n-1}{n^2} \quad (i \neq j), \quad \sum_{i=1}^{n} P_i = \frac{n^2 - n + 1}{n} I$$

and P_i has a constant diagonal. More about this case is in the next section. □

3 Existence of some conditional SIC-POVMs

Theorem 1 tells that conditional SIC-POVMs are the optimal measurements if they exist, but it was not written anything about the existence of such POVMs. The existence of SIC-POVMs for arbitrary dimension is not known and they are a special case of the conditional SIC-POVMs. We can not expect to give a full description of SIC-POVMs, but this section contains a particular example. There are seqveral equiangular frames with less than n^2 projections [3], but it is not clear, what parameters are spanned by their complementary part, ie. what the known parameters are. Intuition suggests that the case when the known part corresponds to a subalgebra of the full matrixalgebra is especially interesting.

Suppose we know the diagonal elements of a n-dimensional density matrix. We want to construct the related conditional SIC-POVM, that is subnormalized projections P_i forming a symmetric POVM and complementary to the diagonal projections $E_i = |e_i\rangle\langle e_i| \in M_n(\mathbb{C})$ $(1 \le i \le n)$. These projections form a maximal abelian subalgebra. Easy dimension counting shows, that we want to construct $N = n^2 - n + 1$ such projections.

So $\{|e_i\rangle : 1 \le i \le n\}$ is an orthonormal basis in the space. We set

$$|\phi\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |e_i\rangle, \qquad q = e^{2\pi \mathrm{i}/N} \tag{10}$$

and a diagonal unitary

$$U = \mathrm{Diag}\,(q^{\alpha_1}, q^{\alpha_2}, q^{\alpha_3}, \dots q^{\alpha_n}),$$

where the integer numbers $0 \le \alpha_i \le N-1$ are differents. Another unitary T permutes the eigenvectors of U:

$$T|e_i\rangle = \begin{cases} |e_{i+1}\rangle & \text{if } 1 \le i \le n-1, \\ |e_1\rangle & \text{if } i = n. \end{cases}$$

Note, that $T|\phi\rangle = T^*|\phi\rangle = |\phi\rangle$. We have

$$\begin{aligned} |\langle U^k\phi, e_j\rangle|^2 &= |\langle \phi, (U^*)^k e_j\rangle|^2 = |q^{-k\alpha_j}|^2 |\langle \phi, e_j\rangle|^2 = |\langle \phi, e_j\rangle|^2 \\ &= |\langle \phi, T^{j-1} e_1\rangle|^2 = |\langle (T^*)^{j-1}\phi, e_1\rangle|^2 = |\langle \phi, e_1\rangle|^2 \end{aligned}$$

and the projections $P_k := |U^k\phi\rangle\langle U^k\phi|$ are complementary to the diagonal projections:

$$\mathrm{Tr}\, |U^k\phi\rangle\langle U^k\phi|\, (|e_i\rangle\langle e_i| - I/n) = 0.$$

It is easy to check that

$$\sum_{k=1}^{N} \langle e_i, U^k\phi\rangle\langle U^k\phi, e_j\rangle = \frac{1}{n}\sum_{k=1}^{N} q^{-\alpha_i k} q^{\alpha_j k} = \frac{1}{n}\sum_{k=1}^{N} q^{(\alpha_j - \alpha_i)k} = \frac{N}{n}\delta_{ij},$$

so we obtain

$$\sum_{k=1}^{N} P_k = \frac{N}{n} I$$

and the sum is multiple of I.

We need to choose the numbers $\alpha_1, \alpha_2, \dots, \alpha_n$ such that

$$\mathrm{Tr}\, P_i P_j = |\langle U^i \phi | U^j \phi \rangle|^2 = \frac{1}{n^2} \left| \sum_{m=1}^{n} q^{(j-i)\alpha_m} \right|^2 = \frac{1}{n^2} t$$

is constant when $i \neq j$. From the formulas

$$\sum_j \mathrm{Tr}\, P_i P_j = (N-1) \frac{1}{n^2} t + 1, \qquad \sum_j \mathrm{Tr}\, P_i P_j = \mathrm{Tr} \left(P_i \sum_j P_j \right) = \frac{N}{n}$$

we obtain $t = n - 1$.

Next we use a terminology from the paper [7]. The set $G := \{0, 1, \dots, N-1\}$ is an additive group modulo N. The subset $D := \{\alpha_i : 1 \le i \le n\}$ is a difference set with parameters (N, n, λ) when the set of differences $\alpha_i - \alpha_j$ contains every nonzero element of G exactly λ times. When this holds, then we have

$$\left| \sum_{i=1}^{n} q^{m\alpha_i} \right|^2 = \sum_{i,j=1}^{n} q^{m(\alpha_i - \alpha_j)} = n + \sum_{s=1}^{N-1} \lambda q^s = n - \lambda,$$

where q is from (10). Here $\lambda = 1$. If the appropriate difference set exists, then there exists a conditional SIC-POVM. Similar constructions of tight equiangular frames related to difference sets are examined in detail in [8].

The existence of difference sets with parameters $(N, n, 1)$ is a known problem, named the prime power conjecture [17, 7], and we get the following result:

Theorem 2 *There exists a conditional SIC-POVM with respect to the diagonal part of a density matrix if $n-1$ is a prime power. Then $N = n^2 - n + 1$ and the projection P_i ($1 \le i \le N$) have the properties*

$$\sum_{i=1}^{N} P_i = \frac{N}{n} I, \qquad \mathrm{Tr}\, P_i P_j = \frac{n-1}{n^2} \quad (i \neq j).$$

A few examples about $M = \{\alpha_k : k\}$ is written here:

$$n = 2, \quad M = \{0, 1\}, \qquad n = 3, \quad M = \{0, 1, 3\},$$

$$n = 4, \quad M = \{0, 1, 3, 9\}, \qquad n = 5, \quad M = \{0, 1, 4, 14, 16\}.$$

References

[1] D. M. Appleby, SIC-POVMs and MUBs: Geometrical relationships in prime dimension, *Foundations of probability and physics 5*, 223–232, AIP Conf. Proc., 1101, Amer. Inst. Phys., New York, (2009).

[2] D. M. Appleby, A. Ericsson and C. A. Fuchs, Properties of QBist state spaces, Foundations of Physics **41**, 564-579, (2011).

[3] B. G. Bodmann, V. I. Paulsen, M. Tomforde, Equiangular tight frames from complex Seidel matrices containing cube roots of unity, Linear Alg. Appl. **430**, 396-417 (2008).

[4] S. Colin, J. Corbett, T. Durt and D. Gross, About SIC POVMs and discrete Wigner Distributions, J. Opt. B: Quantum Semiclass. Opt. **7**, S778 (2005).

[5] G. M. D'Ariano, P. Perinotti and M. F. Sacchi, Informationally complete measurements and groups representation, J. Opt. B **6**, S487 (2004).

[6] S. T. Flammia, On SIC-POVMs in prime dimensions, J. Phys. A: Math. Gen. **39**, 13483 (2006).

[7] D. M. Gordon, The prime power conjecture is true for $n < 2.000.000$, Electronic J. Combinatorics 1, No. 1, R6, 1-7, (1994).

[8] D. Kalra, Complex equiangular cyclic frames and erasures, Linear Algebra and its Applications **419**, 373-399 (2006).

[9] A. Klappenecker, and M. Rötteler, Mutually unbiased bases are complex projective 2-designs, Proc. 2005 IEEE International Symposium on Information Theory, Adelaide, Australia, pages 1740–1744 (2005).

[10] M. Paris and J. Řeháček, *Quantum State Estimation*, Springer-Verlag, Berlin, 2004.

[11] D. Petz and L. Ruppert, Efficient quantum tomography for qubits, to be published.

[12] D. Petz and L. Ruppert, Efficient quantum tomography needs complementary and symmetric measurements, to be published in Rep. Math. Phys.

[13] D. Petz, A. Szántó and M. Weiner, Complementarity and the algebraic structure of four-level quantum systems, J. Infin. Dim. Analysis Quantum Prob., **12**, 1–18 (2009).

[14] J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. **45**, 2171 (2004).

[15] A. J. Scott, Tight informationally complete quantum measurements, J. Phys. A: Math. Gen. **39**, 13507 (2006).

[16] A. J. Scott and M. Grassl, SIC-POVMs: A new computer study, J. Math. Phys. **51**, 042203 (2010).

[17] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc, **43**, 377–385 (1938).

[18] G. Zauner, Quantendesigns - Grundzüge einer nichtkommutativen Designtheorie, PhD thesis (University of Vienna, 1999).

[19] H. Zhu, SIC POVMs and Clifford groups in prime dimensions, J. Phys. A: Math. Theor. **43**, 305305 (2010).